53. (New) A method as recited in claim 52, further comprising:

checking whether the destination computing device is trusted to receive the data; and

preventing the data from being transferred if the destination computing device is not trusted to receive the data.

54. (New) A method as recited in claim 52, wherein checking whether the data can be transferred comprises checking whether the data is non-migrateable, user-migrateable, or third party-migrateable.

A1

55. (New) A method as recited in claim 54, further comprising:

if the data is non-migrateable, then not allowing the data to be transferred;

if the data is user-migrateable, then allowing the data to be transferred under control of a user; and

if the data is third party-migrateable, then allowing the data to be transferred under control of a third party.

56. (New) A method as recited in claim 52, further comprising:

allowing data for a plurality of applications to be transferred to the destination computing device by moving a single key to the destination computing device.

57. (New) A method as recited in claim 52, wherein the data comprises an operating system secret.

58. (New) A method as recited in claim 52, wherein the data comprises a trusted core secret.

59. (New) One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to:

A1

receive a request to transfer data from the source computing device to a destination computing device;

identify a type of the data;

if the type is non-migrateable, then not allow the data to be transferred;

if the type is user-migrateable, then allow the data to be transferred under control of a user; and

if the type is third party-migrateable, then allow the data to be transferred under control of a third party.

60. (New) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the user comprises a plurality of instructions to:

encrypt an encryption key previously used to encrypt the data; and

allow the encrypted encryption key to be copied to the destination computing device.

61. (New) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the user comprises a plurality of instructions to:

identify a user passphrase;

identify an encryption key previously used to encrypt the data, wherein the encryption key corresponds to the user-migrateable type;

encrypt the encryption key based at least in part on the user passphrase; and

allow the encrypted encryption key to be copied to the destination computing device.

A1

62. (New) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the third party comprises a plurality of instructions to:

encrypt an encryption key previously used to encrypt the data; and

allow the encrypted encryption key to be copied to the destination computing device.

63. (New) One or more computer readable media as recited in claim 59, wherein the plurality of instructions to allow the data to be transferred under control of the third party comprises a plurality of instructions to:

identify a public key of a public-private key pair associated with the third party;

identify an encryption key previously used to encrypt the data, wherein the encryption key corresponds to the third party-migrateable type;

encrypt the encryption key based at least in part on the public key; and

allow the encrypted encryption key to be copied to the destination computing device.

64. (New) One or more computer readable media as recited in claim 59, wherein the plurality of instructions further cause the one or more processors to:

A1

authenticate the destination computing device as being trusted to receive the data; and

preventing the data from being transferred if the destination computing device is not trusted to receive the data.

65. (New) One or more computer readable media as recited in claim 59, wherein the plurality of instructions further comprise instructions that cause the one or more processors to:

allow multiple data to be transferred under control of the user by using a single key associated with the user-migrateable type.

66. (New) One or more computer readable media as recited in claim 59, wherein the data comprises an operating system secret.

67. (New) One or more computer readable media as recited in claim 59, wherein the data comprises a trusted core secret.

A1

68. (New) One or more computer readable media having stored thereon a plurality of instructions for backing up data on a computing device, wherein the plurality of instructions, when executed by one or more processors of the computing device, causes the one or more processors to:

check, for data to be backed up, a type of the data;

if the data type is non-migrateable, then not allow the data to be transferred to a backup medium;

if the data type is user-migrateable, then allow the data to be transferred to the backup medium under control of a user; and

if the data type is third party-migrateable, then allow the data to be transferred to the backup medium under control of a third party.

69. (New) One or more computer readable media as recited in claim 68, wherein the instructions to allow the data to be transferred to the backup medium under control of the user further cause the one or more processors to:

encrypt the data based at least in part on a passphrase before the data is transferred to the backup medium.

70. (New) One or more computer readable media as recited in claim 68, wherein the instructions to allow the data to be transferred to the backup medium under control of the user, cause the one or more processors to:

encrypt an encryption key previously used to encrypt the data; and

allow the encrypted encryption key to be transferred to the backup medium.

71. (New) One or more computer readable media as recited in claim 68, wherein the instructions to allow the data to be transferred to the backup medium under control of the user, cause the one or more processors to:

identify a user passphrase;

identify an encryption key previously used to encrypt the data, wherein the encryption key corresponds to the user-migrateable type;

encrypt the encryption key based at least in part on the user passphrase; and

allow the encrypted encryption key to be transferred to the backup medium.

72. (New) One or more computer readable media as recited in claim 68, wherein the instructions to allow the data to be transferred to the backup medium under control of the third party, cause the one or more processors to:

encrypt an encryption key previously used to encrypt the data; and

allow the encrypted encryption key to be transferred to the backup medium.

73. (New) One or more computer readable media as recited in claim 68, wherein the instructions to allow the data to be transferred to the backup medium under control of the third party, cause the one or more processors to:

identify a public key of a public-private key pair associated with the third party;

identify an encryption key previously used to encrypt the data, wherein the encryption key corresponds to the third party-migrateable type;

encrypt the encryption key based at least in part on the public key; and

allow the encrypted encryption key to be transferred to the backup medium.

74. (New) One or more computer readable media as recited in claim 68, wherein the data comprises an operating system secret.

75. (New) One or more computer readable media as recited in claim 68, wherein the data comprises a trusted core secret.

76. (New) A method comprising:

receiving a request to transfer a plurality of secrets from a source computing device to a destination computing device;

identifying which one of a plurality of types of secrets the plurality of secrets correspond to;

identifying a key associated with the one type; and

allowing the plurality of secrets to be accessible to the destination computing device by communicating the key to the destination computing device.

77. (New) A method as recited in claim 76, wherein the type of secret is all secrets and the key associated with the one type is a gatekeeper storage key.

A1 Cont.

78. (New) A method as recited in claim 76, wherein the plurality of secrets comprises one or more operating system secrets.

79. (New) A method as recited in claim 76, wherein the plurality of secrets comprises one or more trusted core secrets.